In the Claims:

1. (Currently amended) An asymmetrical key cryptography method involving a keyholder having a number $m \geq 1$ of private keys $Q_1, Q_2, ..., Q_m$ and respective public keys $G_1, G_2, ..., G_m$, each pair of keys (Q_i, G_i) (where $i = 1, ..., m$) satisfying either the relationship $G_i = Q_i^v \bmod n$ or the relationship $G_i \times Q_i^v = 1 \bmod n$, where n is a public integer equal to the product of f (where $f > 1$) private prime factors $p_1, ..., p_f$, at least two of which are separate, and the exponent v is a public integer equal to a power of 2, wherein the method comprises the steps of: ~~which method is characterized in that~~

arranging exponent v to have the relationship $v = 2^{b+k}$,

where k is a strictly positive integer and $b = \max(b_1, ..., b_f)$, where b_j (where $j = 1, ..., f$) is the highest integer such that $(p_j - 1)/2^{b_j - 1}$ is even; [[,]] and

arranging each public key G_i (where $i = 1, ..., m$) ~~is of~~ to have the form $G_i = g_i^{2^{a_i}} \bmod n$, where the base numbers g_i are integers strictly greater than 1 and the numbers a_i are integers such that $1 \leq a_i \leq b$ and at least one of them is strictly greater than 1.

2. (Currently amended) A method according to claim 1, ~~characterized in that~~ wherein at least one of said prime factors $p_1, ..., p_f$ is congruent to 1 modulo 4 and the integers a_i (where $i = 1, ..., m$) are all equal to said number b.

3. (Currently amended) A method according to claim 1 ~~or claim 2, characterized in that~~ , wherein said base numbers $g_1,...,g_m$ include at least one number g_s and said prime factors $p_1,...,p_f$ include at least two numbers p_t and p_u other than 2 such that, given said numbers $b_1,...,b_f$,

if $b_t = b_u$, then $(g_s | p_t) = -(g_s | p_u)$, and

if $b_t < b_u$, then $(g_s | p_u) = -1$,

where $(g_s | p_t)$ and $(g_s | p_u)$ denote the Legendre symbols of g_s relative to p_t and p_u.

4. (Currently amended) A method according to claim 1, wherein ~~any one of the preceding claims, characterized in that~~ the base numbers $g_1,...,g_m$ are prime numbers.

5. (Currently amended) A method according to claim 1 ~~any one of claims 1 to 4~~, involving a controller and said keyholder, here called the claimant, ~~characterized in that it~~ wherein the method comprises the following steps:

the claimant chooses at random an integer r, calculates the witness $R = r^v \bmod n$ and sends the witness to the controller,

the controller chooses at random m challenges $d_1, d_2,...,d_m$ ~~where $i = 1,...,m$~~ and sends the challenges to the claimant,

the claimant calculates the response

$$D = r \times Q_1^{d_1} \times Q_2^{d_2} \times ... \times Q_m^{d_m} \bmod n,$$

and sends the response to the controller, and

the controller calculates

$D^v \times G_1^{\varepsilon_1 d_1} \times G_2^{\varepsilon_2 d_2} \times ... \times G_m^{\varepsilon_m d_m} \mod n$

where, for $i = 1,...,m$, $\varepsilon_i = +1$ if $G_i \times Q_i^v = 1 \mod n$ and $\varepsilon_i = -1$ if $G_i = Q_i^v \mod n$,

and verifies that the result is equal to the witness R.

6. (Currently amended) A method according to claim 1 ~~any one of claims 1 to 4~~, enabling a controller to verify that a message M that it has received was sent to it by said keyholder, here called the claimant, ~~characterized in that it~~ wherein the method comprises the following steps:

the claimant chooses at random an integer r and first calculates the witness $R = r^v \mod n$, then calculates the token $T = h(M, R)$, where h is a hashing function, and finally sends the token T to the controller,

the controller chooses at random m challenges $d_1, d_2, ..., d_m$ where $i = 1,...,m$, and sends the challenges to the claimant,

the claimant calculates the response

$D = r \times Q_1^{d_1} \times Q_2^{d_2} \times ... \times Q_m^{d_m} \mod n$ and sends the response to the controller, and

the controller calculates $h\left(M, D^v \times G_1^{\varepsilon_1 d_1} \times G_2^{\varepsilon_2 d_2} \times ... \times G_m^{\varepsilon_m d_m} \mod n\right)$ where, for $i = 1,...,m$, $\varepsilon_i = +1$ if $G_i \times Q_i^v = 1 \mod n$ and $\varepsilon_i = -1$ if $G_i = Q_i^v \mod n$, and verifies that the result is equal to the token T.

7. (Currently amended) A method according to claim 5, wherein ~~or claim 6, characterized in that~~ the challenges satisfy the condition $0 \le d_i \le 2^k - 1$ for $i = 1,...,m$.

8. (Currently amended) A method according to claim 1 ~~any one of claims 1 to 4~~, enabling said keyholder, here called the signatory, to sign a message M that it sends to a controller, ~~characterized in that it~~ wherein the method comprises the following steps:

the signatory chooses at random m integers r_i, where $i = 1,...,m$, and first calculates the witnesses $R = r^v \bmod n$, then calculates the token $T = h(M, R_1, R_2, ..., R_m)$, where h is a hashing function producing a word of m bits, and finally sends the token T to the controller,

the signatory identifies the bits $d_1, d_2, ..., d_m$ of the token T,

the signatory calculates the responses $D_i = r_i \times Q_i^{d_i} \bmod n$ and sends the responses to the controller, and

the controller calculates

$$h\left(M, D_1^{\,v} \times G_1^{\varepsilon_1 d_1} \bmod n, D_2^{\,v} \times G_2^{\varepsilon_2 d_2} \bmod n, ..., D_m^{\,v} \times G_m^{\varepsilon_m d_m} \bmod n\right)$$

where, for $i = 1,...,m$, $\varepsilon_i = +1$ if $G_i \times Q_i^v = 1 \bmod n$ and $\varepsilon_i = -1$ if $G_i = Q_i^v \bmod n$, and verifies that the result is equal to the token T.

9. (Currently amended) An electronic circuit including a processor and memories, ~~characterized in that it~~ wherein the electronic circuit can be programmed to act as said keyholder in executing a method according to claim 1 ~~any one of claims 1 to 8~~.

10. (Currently amended) A dedicated electronic circuit, ~~characterized in that it includes~~ including microcomponents enabling ~~it~~ the electronic circuit to process data in such manner as to act as said keyholder in executing a method according to claim 1 ~~any one of claims 1 to 8~~.

11. (Currently amended) A portable object adapted to be connected to a terminal to exchange data with that terminal, ~~characterized in that it~~ wherein the portable object includes an electronic circuit according to claim 9 ~~or claim 10~~ and is adapted to store identification data and private keys specific to said key holder.

12. (Currently amended) A terminal adapted to be connected to a portable object to exchange data with that portable object, ~~characterized in that it~~ wherein the terminal includes a data processing device programmed to act as said controller in executing a method according to claim 1 ~~any one of claims 1 to 8~~.

13. (Currently amended) A cryptography system comprising:

a portable object ~~according to claim 11~~ adapted to be connected to a terminal to exchange data with that terminal, wherein the portable object includes an electronic circuit having a processor and memories, wherein the electronic circuit can be programmed to act as said keyholder in executing a method according to claim 1, and wherein the portable object is adapted to store identification data and private keys specific to said key holder; and

a terminal ~~according to claim 12~~ adapted to be connected to the portable object to exchange data with that portable object, wherein the terminal includes a data processing device programmed to act as said controller in executing a method according to claim 1.

14. (Currently amended) Non-removable data storage means containing electronic data processing program code instructions for, as said keyholder, executing the steps of any of the methods of a method according to claim 1 ~~any one of claims 1 to 8~~.

15. (Currently amended) Partially or totally removable storage means containing electronic data processing program code instructions for, as said keyholder, executing the steps of a method according to claim 1 ~~any one of claims 1 to 8~~.

16. (Currently amended) A data processing device comprising storage means according to claim 14 ~~or claim 15~~.

17. (Currently amended) Non-removable data storage means containing electronic data processing program code instructions for, as said controller, executing the steps of any of the methods of a method according to claim 1 ~~any one of claims 1 to 8~~.

18. (Currently amended) Partially or totally removable data storage means containing electronic data processing program code instructions for, as said controller, executing the steps of a method according to claim 1 ~~any one of claims 1 to 8~~.

19. (Currently amended) A data processing device, ~~characterized in that~~ wherein it comprises storage means according to claim 17 ~~or claim 18~~.

20. (Currently amended) A cryptography system comprising:

a data processing device ~~according to claim 16~~ including non-removable storage means containing electronic data processing program code instructions for, as said keyholder, executing the steps of any of the methods of a method according to claim 1; and

a data processing device ~~according to claim 19~~ including non-removable data storage means containing electronic data processing program code instructions for, as said controller, executing the steps of any of the methods of a method according to claim 1.

21. (Currently amended) A computer program containing instructions such that, when said program controls a programmable data processing device, said instructions cause said data processing device to execute a method according to claim 1 ~~any one of claims 1 to 8~~.

22. (New) A method according to claim 4, wherein the base numbers $g_1,...,g_m$ are chosen from the first 54 prime numbers.